1/10

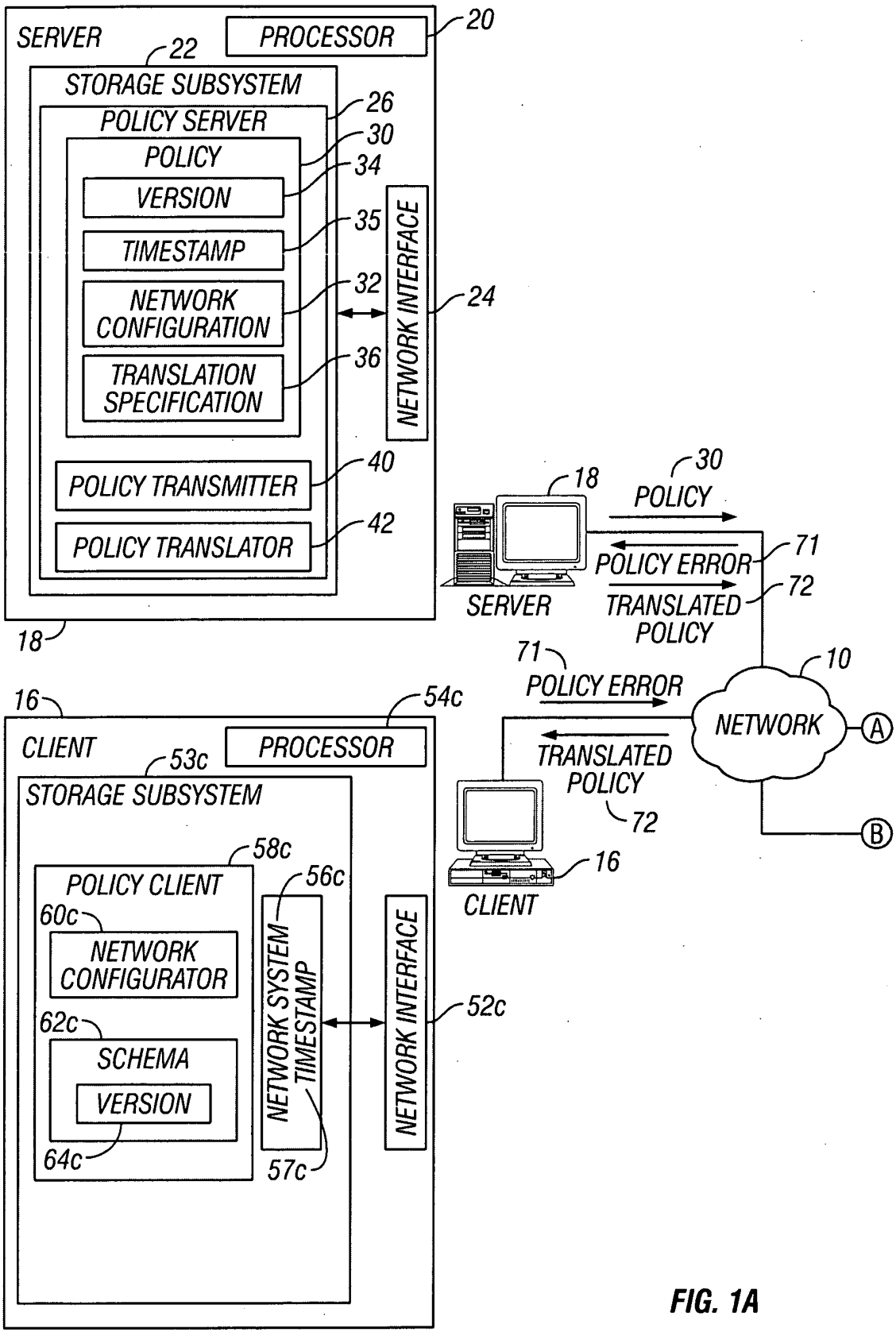


FIG. 1A

2/10

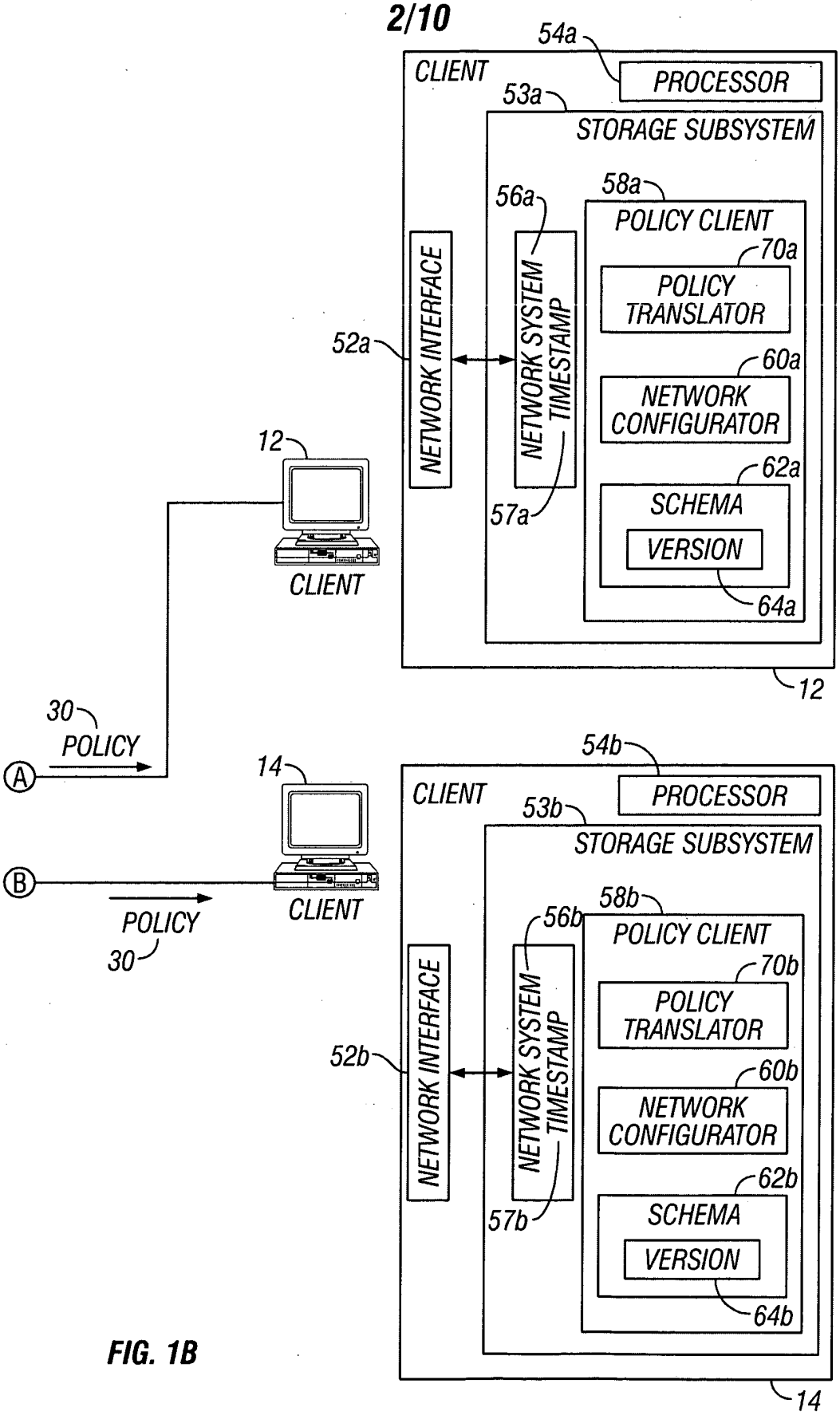
54a
CLIENT
PROCESSOR
53a
STORAGE SUBSYSTEM
58a
56a
POLICY CLIENT
70a
POLICY TRANSLATOR
NETWORK INTERFACE
NETWORK SYSTEM TIMESTAMP
52a
60a
NETWORK CONFIGURATOR
62a
SCHEMA
VERSION
57a
64a
12
CLIENT
30
POLICY
A
B
14
54b
CLIENT
PROCESSOR
53b
STORAGE SUBSYSTEM
58b
56b
POLICY CLIENT
70b
POLICY TRANSLATOR
NETWORK INTERFACE
NETWORK SYSTEM TIMESTAMP
52b
60b
NETWORK CONFIGURATOR
62b
SCHEMA
VERSION
57b
64b
14

FIG. 1B

```
// Policy that conforms to the newer schema (specifies Rjindael):                    30

<?xml version="1.0"?>

<!DOCTYPE IPsecPolicyOnSystem PUBLIC "//somestandard.org/IPsecPolicy/Version1.1">   34

<IPsecPolicyOnSystem timestamp="2000-9-30_12:12:12">                               35

    <IKEProposals>
                                                94a        96a        98a          92a
90a <IKEProposal id="Proposal1" CipherAlgorithm="DES" HashAlgorithm="MD5" GroupId="DH768" AuthenticationMethod="Preshared"/>
                                                94b        96b        98b          92b
90b <IKEProposal id="Proposal2" CipherAlgorithm="Rjindael" HashAlgorithm="SHA-1"  GroupId="DH1024" AuthenticationMethod="DSS_Signatures"/>

    </IKEProposals>

</IPsecPolicyOnSystem>
```

32 / 90

FIG. 2

```
// DTD schema Version 1.1 for IPsec implementations that support the new
// encryption algorithm called Rjindael:                                    100

<?xml version="1.0" encoding="UTF-16"?>

<!ELEMENT IKEProposal EMPTY>

<!ATTLIST IKEProposal
   102 id ID #REQUIRED 104                                                  110
   108 CipherAlgorithm (3DES | DES | IDEA | Blowfish | RC5 | CAST | Rjindael) #REQUIRED 112
   114 HashAlgorithm (MD5 | SHA-1 | Tiger) #REQUIRED                        120
   116 GroupId (DH768 | DH1024 | DH1536 | ECC2N155 | ECC2N185) #REQUIRED   122
   118 AuthenticationMethod (DSS_Signatures | Preshared | RSA_Signatures |
       RSA_Encryption | Revised_RSA_Encryption | Kerberos) #REQUIRED        124
>                                                                           101

<!ELEMENT IKEProposals (IKEProposal+)>

<!ELEMENT IPsecPolicyOnSystem (IKEProposals)>

<!ATTLIST IpsecPolicyOnSystem
      timestamp CDATA #REQUIRED 126
>
```

FIG. 3

```
// DTD schema for version 1.0 IPsec policy implementations (doesn't
// include the new encryption algorithm called Rjindael):

<?xml version="1.0" encoding="UTF-16"?>

<!ELEMENT IKEProposal EMPTY>

<!ATTLIST IKEProposal

    id ID #REQUIRED

    CipherAlgorithm (3DES | DES | IDEA | Blowfish | RC5 | CAST) #REQUIRED

    HashAlgorithm (MD5 | SHA-1 | Tiger) #REQUIRED

    GroupId (DH768 | DH1024 | DH1536 | ECC2N155 | ECC2N185) #REQUIRED

    AuthenticationMethod (DSS_Signatures | Preshared | RSA_Signatures |

    RSA_Encryption | Revised_RSA_Encryption | Kerberos) #Required
>
<!ELEMENT IKEProposals (IKEProposal+)>

<!ELEMENT IPsecPolicyOnSystem (IKEProposals)>

<!ATTLIST  IPsecPolicyOnSystem

    timestamp CDATA #REQUIRED
>
```

130

132

134

FIG. 4

**6/10**

36

```
// XSLT file to transform the above policy into a policy conforming to the older
// schema. This transformation simply replaces attribute "Rjindael" with "3DES".

<?xml version="1.0" encoding="UTF-8"?>
<!-- This stylesheet replaces the CipherAlgorithm Rjindael with 3DES, for IKE
implementations that do not support Rjindael. -->
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
    <xsl:output method="xml" version="1.0" encoding="UTF-8" indent="yes"/>

    <xsl:output doctype-public-"//somestandard.org/IPsecPolicy/Version1.0"/>   146

        <xsl:template match="/*">
    <xsl:element name="IPsecPolicyOnSystem">
    <xsl:copy-of select="@*"/>
    <xsl:element name="IKEProposals">
    <xsl:apply-templates select="IKEProposals"/>
    </xsl:element>
    </xsl:element>
    </xsl:template>

    <xsl:template match="IKEProposals/IKEProposal">

        <xsl:element name="IKEProposal">
            <xsl:copy-of select="@*"/>
            <xsl:if test="@CipherAlgorithm = 'Rjindael'">   142a
142         <xsl:attribute name="CipherAlgorithm">3DES</xsl:attribute>   142b
            </xsl:if>

        </xsl:element>

    </xsl:template>

</xsl:stylesheet>
```

**FIG. 5A**

```
// Output resulting from applying the above transformation to the policy:
<?xml version="1.0" encoding="utf-8"?>                                    72
<!DOCTYPE IPsecPolicyOnSystem PUBLIC "//somestandard.org/IPsecPolicy/Version1.0">   150
<IPsecPolicyOnSystem timestamp="2000-9-30_12:12:12">                      35
<IKEProposals>
   <IKEProposal id="Proposal1" CipherAlgorithm="DES" HashAlgorithm="MD5" GroupId="DH768" AuthenticationMethod="Preshared"/>
   <IKEProposal id="Proposal2" CipherAlgorithm="3DES" HashAlgorithm="SHA-1" GroupId="DH1024" AuthenticationMethod="DSS_Signatures"/>   160
</IKEProposals>
</IPsecPolicyOnSystem>
```

FIG. 5B

**8/10**

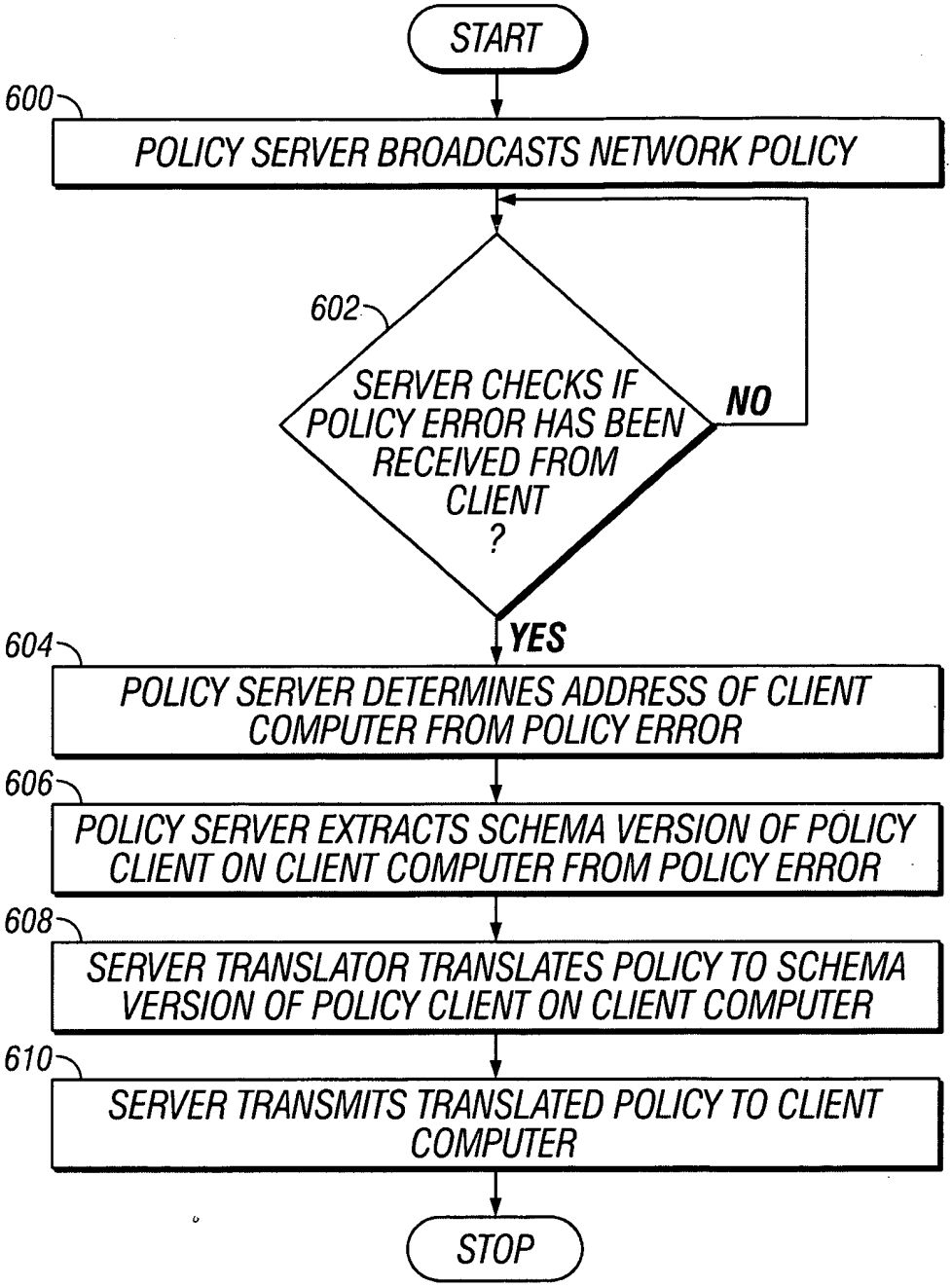
START
600
POLICY SERVER BROADCASTS NETWORK POLICY
602
SERVER CHECKS IF POLICY ERROR HAS BEEN RECEIVED FROM CLIENT ?
NO
YES
604
POLICY SERVER DETERMINES ADDRESS OF CLIENT COMPUTER FROM POLICY ERROR
606
POLICY SERVER EXTRACTS SCHEMA VERSION OF POLICY CLIENT ON CLIENT COMPUTER FROM POLICY ERROR
608
SERVER TRANSLATOR TRANSLATES POLICY TO SCHEMA VERSION OF POLICY CLIENT ON CLIENT COMPUTER
610
SERVER TRANSMITS TRANSLATED POLICY TO CLIENT COMPUTER
STOP

**FIG. 6**

**9/10**

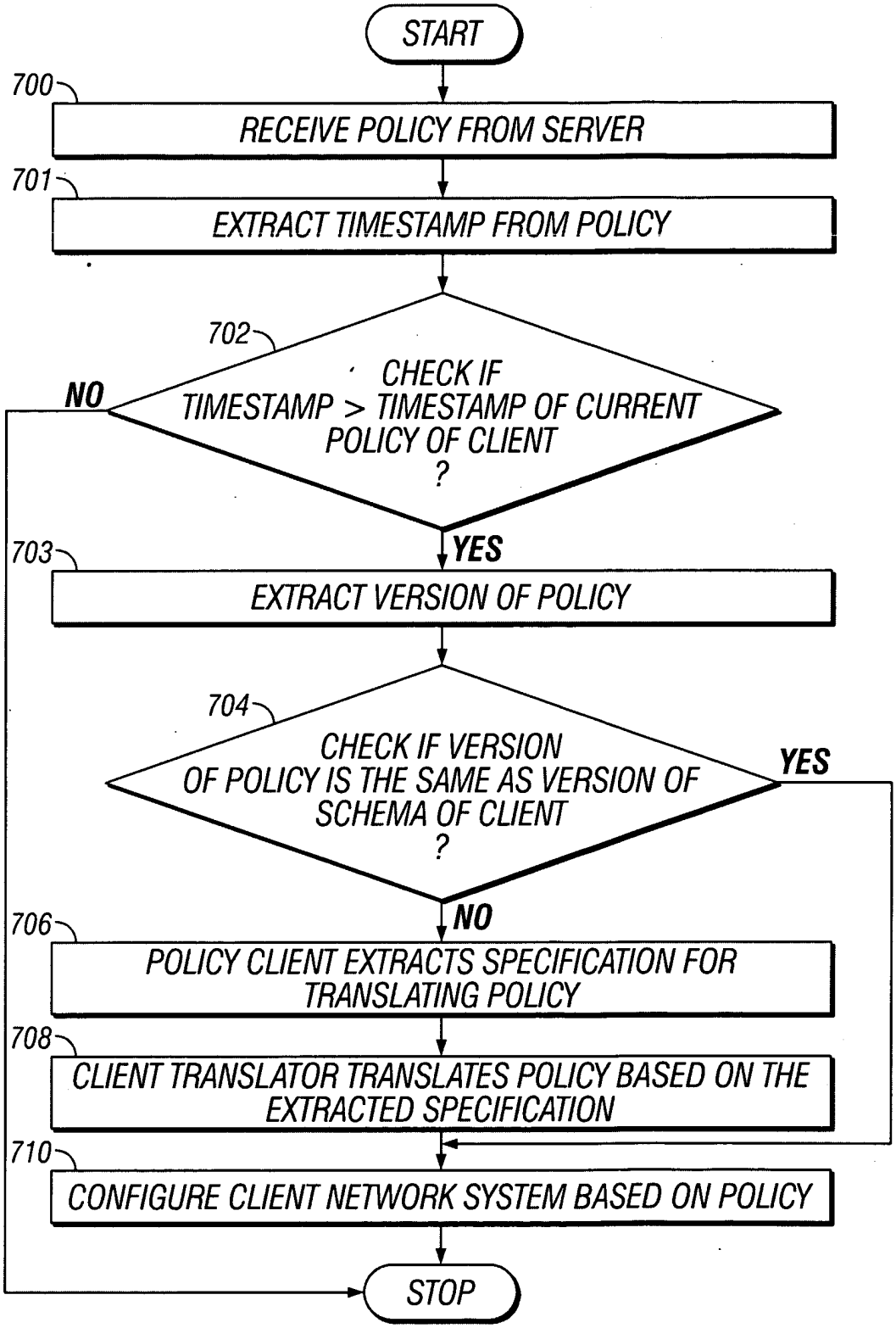
START
700
RECEIVE POLICY FROM SERVER
701
EXTRACT TIMESTAMP FROM POLICY
702
CHECK IF TIMESTAMP > TIMESTAMP OF CURRENT POLICY OF CLIENT ?
NO
YES
703
EXTRACT VERSION OF POLICY
704
CHECK IF VERSION OF POLICY IS THE SAME AS VERSION OF SCHEMA OF CLIENT ?
YES
NO
706
POLICY CLIENT EXTRACTS SPECIFICATION FOR TRANSLATING POLICY
708
CLIENT TRANSLATOR TRANSLATES POLICY BASED ON THE EXTRACTED SPECIFICATION
710
CONFIGURE CLIENT NETWORK SYSTEM BASED ON POLICY
STOP

FIG. 7A

**10/10**

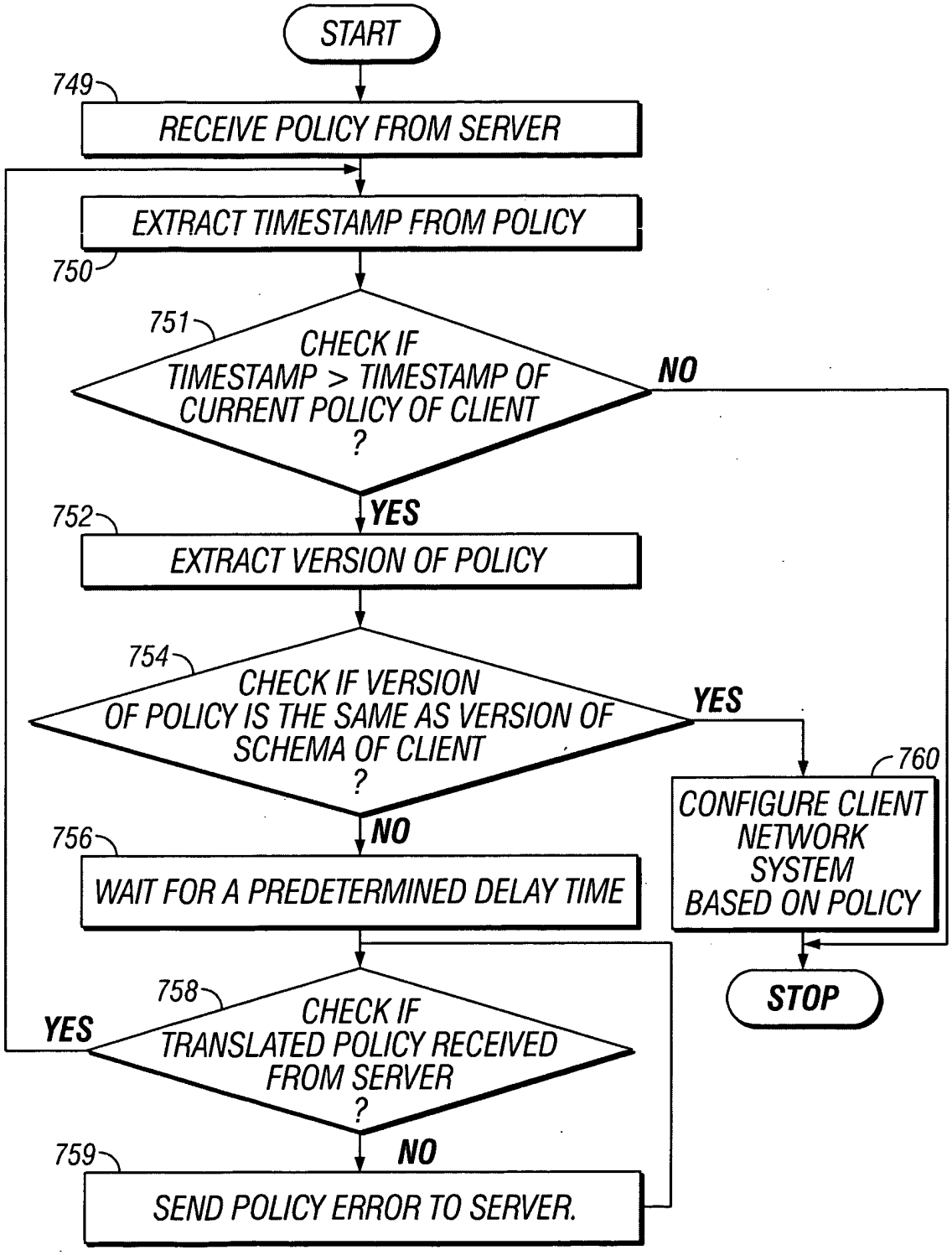
START
749
RECEIVE POLICY FROM SERVER
EXTRACT TIMESTAMP FROM POLICY
750
751
CHECK IF TIMESTAMP > TIMESTAMP OF CURRENT POLICY OF CLIENT ?
NO
YES
752
EXTRACT VERSION OF POLICY
754
CHECK IF VERSION OF POLICY IS THE SAME AS VERSION OF SCHEMA OF CLIENT ?
YES
760
CONFIGURE CLIENT NETWORK SYSTEM BASED ON POLICY
NO
756
WAIT FOR A PREDETERMINED DELAY TIME
STOP
758
CHECK IF TRANSLATED POLICY RECEIVED FROM SERVER ?
YES
NO
759
SEND POLICY ERROR TO SERVER.

FIG. 7B